UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,438	07/08/2003	Patricia Ann Jakubik	RSW920030078US1	7454

36736 7590 08/13/2007

DUKE W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
FRINK, JOHN MOORE	
ART UNIT	**PAPER NUMBER**
2142	
MAIL DATE	**DELIVERY MODE**
08/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/615,438	JAKUBIK ET AL.	
	Examiner	Art Unit	
	John M. Frink	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krumel (US 2002/0083331 A1) in view of Mimura et al. (US 6,847,613 B2), hereafter Mimura, further in view of Aoki et al. (6,757,255 B1), hereafter Aoki, further in view of March et al. (US 2003/0043740 A1), hereafter March.

3. Regarding claim 1, Krumel shows a method of detecting a denial of service attack at a network server (Fig. 18), including being responsive to the number of packets in a specified interval exceeding a specified minimum [0009-0011, 0071-0073, 0082-0084], and setting a denial of service event marker ([0108-0109]).

Krumel does not show counting the number of inbound packets and a number of discarded packets in a specified interval.

Mimura shows counting the number of inbound packets and a number of discarded packets in a specified interval (col. 7 lines 1 – 16).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel with that of Mimura in order to enable collecting and thus displaying more information about current system conditions to users, allowing said users to make more informed decisions.

Krumel in view of Mimura do not show calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, as a response to the number of discarded packets.

Aoki shows calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets (Fig. 10, col. 9 line 12 – col. 10 line 19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura with that of Aoki in order to express system information related to packet drops in both rates (as shown by Krumel) and percentages, as the are two inherently related, thus enabling providing information to users in a variety of forms.

Krumel in view of Mimura and Aoki do show being responsive to a number of discarded packets, but they do not show where this response is performing a calculation determining a percentage of discarded packets.

The examiner takes official notice that it was notoriously old and well known in the art at the time of the invention that performing an addition step (inherently involved in the tracking of said number of discarded packets) is simpler logically and computationally than calculating a percentage, which requires more complex multiplication/division.

The claimed 'responsive to a number of packets' inherently involves a simple addition step, as tracking the count of a number of items on a computer inherently

utilizes addition. By performing said 'calculating a percentage' responsive to the number of discarded packets, inherently tracked by addition, the simple addition step is performed frequently (each time a packet is discarded) and the complex percentage step is performed rarely (only after a certain number of discards have occurred).

It would have been obvious to one of ordinary skill in the art at the time of the invention to perform said simple arithmetic procedure frequently and said percentage calculating procedure rarely, as that would have the predictable result of lowering processor utilization, thus increasing performance.

It thus would have been obvious to one of ordinary skill in the art at the time of the invention to perform said calculation of a percentage of discarded packets as a response to the number of discarded packets.

Krumel in view of Mimura and Aoki show setting a denial of service marker (Krumel, Fig. 18), but do not show where it is set responsive to the percentage of discarded packets exceeding a specified threshold.

March shows responsive to the percentage of packets exceeding a threshold, a denial of service attack is reported ([97-103]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura and Aoki with that of March in order to accurately report the occurrence of denial of service attacks.

4. Regarding claim 2, Krumel in view of Mimura, Aoki and March further show collecting inbound packet information to further characterize the denial of service attack (Krumel, [108-109], Aoki, Fig. 10, and, specifically where March shows a 'generate

alarm' option that avoids the 'shutdown' option, thus resulting in continuing to gather data (March, Fig. 7, [97-103]).

5. Regarding claim 3, Krumel in view of Mimura, Aoki and March further show initiating a flood monitoring process that is executed at designated intervals to collect the inbound packet information (Mimura, col. 7 lines 1 – 16) while the denial of service attack is in progress (March, [97-103], Krumel, Fig. 18, [108-109]).

6. Claims 4 - 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Krumel in view of Mimura, Aoki and March as applied to claims 1 - 3 above, and further in view of Rabe et al. (US 7,194,538 B1), hereafter Rabe.

7. Regarding claim 4, Krumel in view of Mimura, Aoki and March further show a denial of service marker (Krumel, Fig. 18; Mimura col. 7 lines 1 – 16, Aoki, Fig. 10, col. 9 line 12 – col. 10 line 19) responsive to a number of discarded packets (Krumel [0085,0109], March [0097-0103]).

Krumel in view of Mimura, Aoki and March do not show resetting the denial of service event marker if a number of discarded packets in the specified interval before execution of the flood monitoring process is lower than a second specified minimum.

Rabe shows resetting an alarm after a second specified minimum (in Rabe's case, specified as normal operating conditions) is reached (col. 21 lines 50 – 67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Krumel in view of Mimura, Aoki and March with that of Rabe to prevent an alarm from sounding incessantly as well as to ensure that said alarm was only active when alarm conditions were present.

Krumel in view of Mimura, Aoki and March and Reba do not explicitly show where said monitoring is done in the interval before execution of the flood monitoring process. However, Mimura, as described in the response to claim 2, shows monitoring at all intervals (Fig. 7) unless specifically shut down. It thus would have been obvious to monitor for the packet drop rate to return to normal at all times, including before execution of the flood monitoring process.

8. Regarding claim 5, Krumel in view of Mimura, Aoki, March and Rabe further show resetting the denial of service event marker if a rate of discarded packets (Krumel, [0085,0109]) in the specified interval before execution of the flood monitoring process is less than a second specified threshold (Rabe, col. 21 lines 50 – 67, Mimura, Fig. 7, col. 7 lines 1 – 16, Aoki Fig 10).

9. Regarding claims 6 and 10, Krumel in view of Mimura, Aoki, March and Rabe further show collecting the inbound packet information to further characterize the denial of service attack when the denial of service attack is declared over.

Mimura, as described in the response to claim 2 and further in the response to claim 4, shows monitoring at all intervals (Fig. 7) unless specifically shut down. It thus would have been obvious to monitor inbound packet information at all times, including when the denial of service attack is declared over. Furthermore, it is inherent that data collected just before, during, or after a denial of service attack would characterize said attack, as said data would directly reflect on the conditions just before, during and after said attack. Thus continual data collection at all of said intervals would allow additional information regarding said attack to be gathered.

10. Regarding claim 7, Krumel in view of Mimura, Aoki, March and Rabe further show where inbound packet information includes a number of inbound packets in a last interval (Aoki, Fig. 10 and Mimura, col. 7 lines 1 – 16), a number of discarded packets in a last interval (Aoki, Fig. 10) and a packet discard rate (Aoki, Fig. 10).

11. Regarding claim 8, Krumel in view of Mimura, Aoki, March and Rabe further show determining if the denial of service attack is still in progress by comparing the packets discarded in a last interval with the number of inbound packets (Mimura, col. 6 lines 1 – 16, Krumel [71-73,82-84,108-109]), and maintaining the flood monitoring process if the denial of service attack is still in progress (Rabe, col. 21 lines 50 – 67, specifically showing only turning off the alarm when levels return to normal).

12. Regarding claim 9, Krumel in view of Mimura, Aoki, March and Rabe further show collecting inbound packet information for the last interval (Rabe, col. 21 lines 50 – 67, Aoki, Fig. 10).

Response to Arguments

13. Applicant's arguments with respect to all claims have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. Frink whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Frink

(571) 272-9686

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER